

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-167098
(43)Date of publication of application : 24.06.1997

51)Int.Cl. G06F 11/00
H04B 10/105
H04B 10/10
H04B 10/22
H04L 9/16

21)Application number : 08-194532
22)Date of filing : 24.07.1996

(71)Applicant : HEWLETT PACKARD CO <HP>
(72)Inventor : VARADHARAJAN VIJAY
DACK DAVID GEORGE

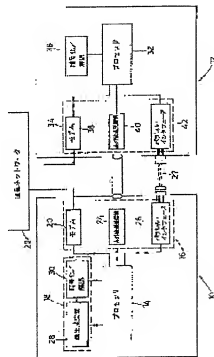
30)Priority
Priority number : 95 95305282 Priority date : 28.07.1995 Priority country : EP

54' COMMUNICATION SYSTEM FOR PORTABLE DEVICE

57)Abstract:

PROBLEM TO BE SOLVED: To improve the safety of a communication network of low safety when a communication is made through the communication network and obtain a security system which is applicable to wide-range use by providing a key update means which allows a host device and a portable device to start sharing a security key or code data and then performs subsequent control over a remote communication and ciphering.

SOLUTION: The portable device 12 and host device 10 exchange the security key periodically through a direct communication link and the key is used to perform the subsequent control over the remote communication and the ciphering. An arbitrary key is used as 1st key and inputted to the host device 10 and portable device 12. For example, the host device 10 and portable device 12 both have the standard code of relatively low safety which is already programmed. A user is instructed so that the key is exchanged as early as possible before the host device 10 is connected to a pay telephone communication network 22. Then, the security key is obtained by exchanging the 1st key.



ル通信を行なうことのできる第1及び第2装置を含む、通信システム内でリモート装置を認証する方法であって、前記第1及び第2装置が互いに近接した場所にあるかどうかを判定し、前記第1及び第2装置が近接した場所にある場合に前記ローカル通信リンクを介して前記装置間でセキュリティ鍵、又はコード・データの共用を開始し、それによって前記装置のうちの少なくとも1つの身分を、前記通信媒体を介した以降のリモート通信において認証することができることを特徴とする前記方法。

【0047】11. 通信媒体を介したリモート通信、又はローカル通信リンクや直接通信リンクを介したローカル通信を行なうことのできる第1及び第2装置を含む、通信システム内でデータを暗号化する方法であって、前記第1及び第2装置が互いに近接した場所にある場合に前記ローカル通信リンクを介した前記装置間でセキュリティ鍵、又はコード・データの共用を開始し、それによって前記通信媒体を介した以降のリモート通信を、前記セキュリティ鍵、又はコード・データを用いて暗号化できることを特徴とする前記方法。

【0048】

【発明の効果】本発明によって、ホスト装置と携帯装置が、安全性の低い通信ネットワークを介して通信する場

合に、その安全性を向上させ、広範な使用に適し、かつ鍵の配布や交換に人畜な制度や信頼される仲介者を必要としないセキュリティ・システムが提供される。

【図面の簡単な説明】

【図1】本発明による通信システムの概略を示すブロック図である。

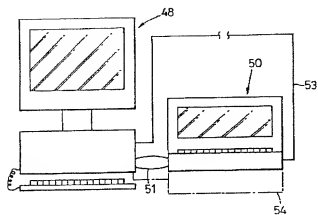
【図2】ホストコンピュータ及びポータブル・コンピュータに適用された本発明の第1の実施例の概略図である。

【図3】通常の電話機とセルラ電話に適用された本発明の第2の実施例の概略図である。

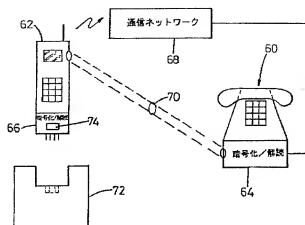
【符号の説明】

- 10 ホスト装置
- 12 携帯装置
- 14、32 プロセッサ
- 16、34 通信モジュール
- 18、36 暗号化/解読モジュール
- 20、38 モデム
- 22 通信ネットワーク
- 24、40 送信機/受信機ユニット
- 26、42 パラレル・インタフェース
- 27 ケーブル・リンク
- 28 鍵生成装置
- 30 暗号化/解読装置

【図2】



【図3】



【图 7】

